FortiAnalyzer Upgrade Guide

VERSION 5.4.0

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

1

Overview

STEP 1: Before You Begin

Make sure FortiAnalyzer 5.4 can run on your FortiAnalyzer model. Back up your device configuration and logs. Wait until all the running reports are completed.

STEP 2: Download

Download upgrade images from Fortinet Customer Service & Support portal.

STEP 3: Upgrade and Monitor

Install the new firmware and monitor if a database rebuild occurs.

STEP 4: Verify

Verify the upgrade has been completed successfully.

2

Upgrade Paths

You can upgrade FortiAnalyzer 5.2.0 or later directly to FortiAnalyzer 5.4.0.

If you are upgrading from versions earlier than 5.2.0, you will need to upgrade to FortiAnalyzer 5.2 first (we recommend that you upgrade to the latest version of FortiAnalyzer 5.2). For information about upgrading to FortiAnalyzer 5.2, see FortiAnalyzer 5.2 Upgrade Guide.

Table 1: FortiAnalyzer 5.4 upgrade paths

Initial Version	Upgrade To	Log Database Rebuild Occurs?
5.0.6–5.0.11	5.2	Yes for 5.0.6, No for the rest
5.2.0 or later	5.4.0	Yes

3

Detailed Upgrade Instructions

Step 1. Before you begin

- Make sure FortiAnalyzer 5.4 can run on your FortiAnalyzer model. For a list of FortiAnalyzer models that support FortiAnalyzer 5.4, see “Supported Models” on page 14.
- Back up your device configuration and logs. See “To back up device configuration” on page 8.
- Wait until all the running reports are completed. Use the following CLI commands to check for running and pending reports.

```
FAZ1000D # dia report status running
FAZ1000D # dia report status pending
```

- If you are upgrading a FortiAnalyzer VM, make sure your VM partition has more than 512MB*, and your VM server is up to date.

To back up device configuration:

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, go to *System Configuration*, and click the *Backup* link.
3. In the *Backup* dialog box that opens, select the *Encryption* check box to enable encryption; enter and confirm the password.
4. Click *OK* and save the backup file on your management computer.

Step 2. Download

To download the firmware image:

1. Log into the Fortinet Customer Service & Support portal at https://support.fortinet.com.
2. On the toolbar, click *Download > Firmware Images* (Figure 1).

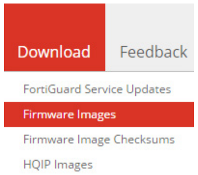
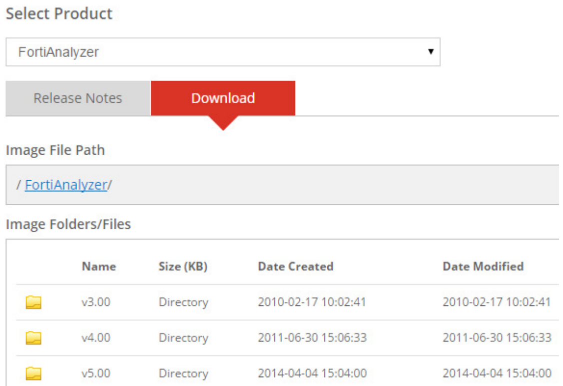


Figure 1: Download menu

3. On the *Select Product* drop-down list, Select *FortiAnalyzer* (Figure 2).



Select Product

FortiAnalyzer

Image File Path

/ FortiAnalyzer/

Image Folders/Files

	Name	Size (KB)	Date Created	Date Modified
	v3.00	Directory	2010-02-17 10:02:41	2010-02-17 10:02:41
	v4.00	Directory	2011-06-30 15:06:33	2011-06-30 15:06:33
	v5.00	Directory	2014-04-04 15:04:00	2014-04-04 15:04:00

Figure 2: Firmware image page

4. Click the *Download* tab, and browse to the folder for version 5.4 (or 5.2.0 if you are upgrading from versions earlier than 5.2.0).

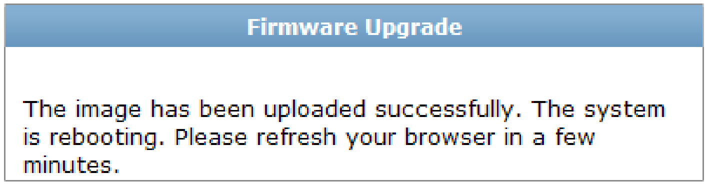
* *We recommend that you allocate 1024MB for the FortiAnalyzer VM partition.*

5. On the image file list, go to the image for your FortiAnalyzer model and click the *HTTPS* link to download the firmware image (.out) to your management computer.
6. To verify the integrity of your download, you can click the *Checksum* link of the image file and compare the checksum code displayed with that of the firmware image you downloaded.
7. Click the *Release Notes* tab, and download the corresponding Release Notes.

Step 3. Upgrade and Monitor

To install the firmware upgrade:

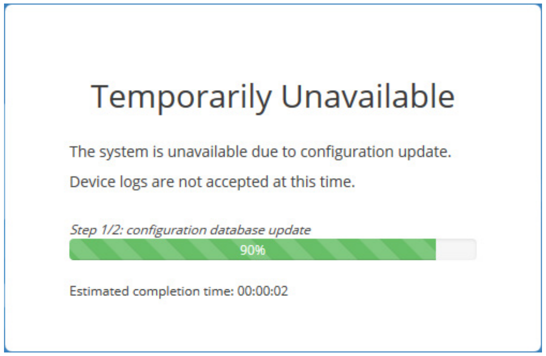
1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, go to the *Firmware Version* field, and click the *Update* link.
3. In the *Firmware Upgrade* dialog box that opens, click *Choose File* and browse to the firmware package (.out file) that you downloaded to the management computer.
4. Click *OK*. Your device will start uploading the firmware image.
5. When you see the following system message (Figure 3), clear the cache of your web browser and keep refreshing the web page.



The image has been uploaded successfully. The system is rebooting. Please refresh your browser in a few minutes.

Figure 3: Firmware upgrade success message

You will then see the new FortiAnalyzer Flat user interface and the system temporarily unavailable message (Figure 4).



The system is unavailable due to configuration update.

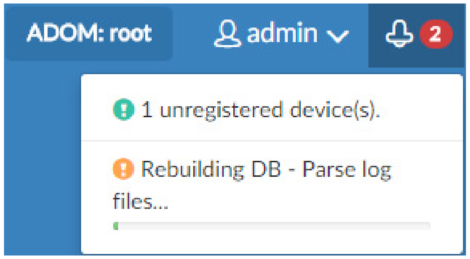
Device logs are not accepted at this time.

Step 1/2: configuration database update

Estimated completion time: 00:00:02

Figure 4. System temporarily unavailable message

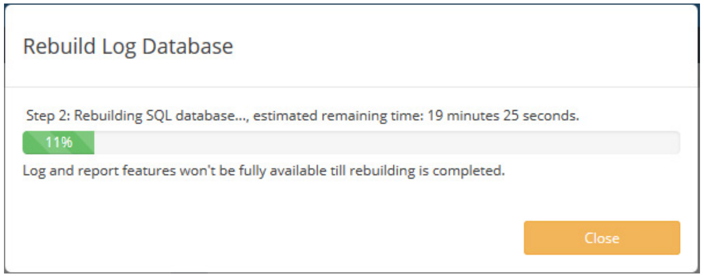
6. Once the Login window is displayed, log into FortiAnalyzer.
7. Select an ADOM.
8. If the database is rebuilding, go to *Notification Center,* and click *Rebuilding DB* status (Figure 5).
9. Monitor the rebuild status. The rebuild process consists of two steps (Figure 6). Eventually, you will see the “Rebuilding log database was completed“ message (Figure 7).



1 unregistered device(s).

Rebuilding DB - Parse log files...

Figure 5: Rebuilding log DB status in Notification Center

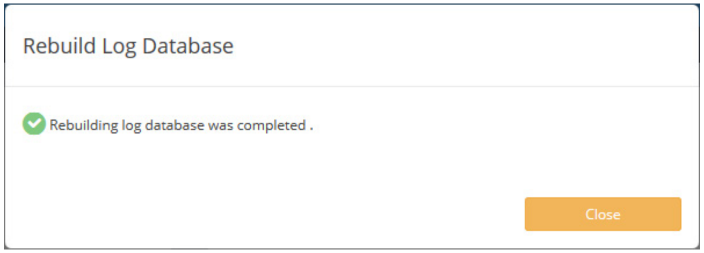


Rebuild Log Database

Step 2: Rebuilding SQL database..., estimated remaining time: 19 minutes 25 seconds.

Log and report features won't be fully available till rebuilding is completed.

Figure 6: Rebuilding log DB–step 2



Rebuild Log Database

Rebuilding log database was completed .

Figure 7: Rebuilding log DB completed message

Not all features are available while the SQL database is being rebuilt.

Step 4. Verify

Verify the following to make sure the upgrade has been completed successfully.

1. Database rebuild is successful, if rebuild occurred.

   Use this CLI command to check database rebuild:

   ```
   diag sql status rebuild-db
   ```

2. Configurations are not lost.
3. Launch the Device Manager module and make sure that all the log devices that were added previously are still listed.
4. Launch other functional modules and make sure they work properly.

By default, the SQL database is disabled for the Collector mode in 5.4 to optimize performance. For a Collector with the SQL database enabled, the SQL database will be disabled after upgrade. You can re-enable the SQL storage settings to view logs and analytics with the following CLI command:

```
config system sql
set status local
end
```

You might want to reconfigure log storage settings after upgrade. Changes have been made in 5.4 to make configuring and monitoring log storage easier, and default values are provided. For details, see the “Configuring log storage” section in *FortiAnalyzer 5.4 Administrator Guide*.

Supported Models

FortiAnalyzer 5.4 can run on the following FortiAnalyzer models:

Table 2: FortiAnalyzer 5.4 supported models

FortiAnalyzer	FortiAnalyzer VM
FAZ-200D	FAZ-VM32
FAZ-300D	FAZ-VM64
FAZ-1000D	FAZ-VM64-AWS
FAZ-2000B	FAZ-VM64-HV
FAZ-3000D	FAZ-VM64-KVM
FAZ-3000E	FAZ-VM64-XEN
FAZ-3500E	
FAZ-3900E	
FAZ-4000B	